```
TED3269
ORIGIN DS-00

INFO  LOG-00   MFA-00   EEB-00   AF-00    A-00     CIAE-00  COME-00
      INL-00   DNI-00   DODE-00  DOTE-00  WHA-00   PERC-00  EAP-00
      DHSE-00  EUR-00   OIGO-00  FAAE-00  FBIE-00  TEDE-00  INR-00
      IO-00    L-00     MFLO-00  MMP-00   MOFM-00  MOF-00   NEA-00
      DCP-00   NSCE-00  OIG-00   PM-00    DOHS-00  FMPC-00  SP-00
      IRM-00   SSO-00   SS-00    USSS-00  CBP-00   R-00     SCRS-00
      PMB-00   DSCC-00  SCA-00   SAS-00   FA-00      /000R

045504
SOURCE: CBLEXCLS.004262
DRAFTED BY: DS/DSS/CC:JBACIGALUPO -- 05/05/2009  571-345-3132
APPROVED BY: DS/DSS/CC:JBACIGALUPO
                  ------------------601CE4  051703Z /38
P 051644Z MAY 09
FM SECSTATE WASHDC
TO SECURITY OFFICER COLLECTIVE PRIORITY
AMEMBASSY TRIPOLI PRIORITY
INFO AMCONSUL CASABLANCA PRIORITY
XMT AMCONSUL JOHANNESBURG
AMCONSUL JOHANNESBURG
```

SECRET STATE 045504

NOFORN

E.O. 12958: DECL: MR
TAGS: ASEC
SUBJECT: DIPLOMATIC SECURITY DAILY

Classified By: Derived from Multiple

SECRET//FGI//NOFORN

Declassify on: Source marked 25X1-human, Date of source: May 4, 2009

¶1. (U) Diplomatic Security Daily, May 5, 2009

¶2. (U) Iraq - Paragraphs 8-13

¶3. (U) Significant Events - Paragraphs 14-20

¶4. (U) Key Concerns - Paragraphs 21-32

¶5. (U) Threats & Analysis - Paragraphs 33-36

¶6. (U) Cyber Threats - Paragraphs 37-45

¶7. (U) Suspicious Activity Incidents - Paragraphs 46-59

¶8. (U) Iraq

¶9. (SBU) One round of indirect fire (IDF) was launched against the International Zone (IZ) in Baghdad at 4:50 a.m. on May 4. An audible explosion was heard in the northeast corner of the U.S. Embassy's construction site. Explosive Ordnance Disposal (EOD) and Regional Security Office react teams responded; the EOD determined a 107 mm rocket impacted. There were no reports of injuries or damage. The "all clear" was given at 5:12 a.m. (RSO Baghdad Spot Report)

¶10. (SBU) Regional Embassy Office (REO) Hillah received IDF from an unknown location May 2 at 11 p.m. Two rounds impacted north and one south of the REO. All personnel were accounted for. Suspected launch sites were identified for further investigation. (RSO Baghdad Spot Report)

¶11. (S//NF) Surveillance of MNF-I and U.S. personnel at BIA: According to multiple-source reporting, Multi-National Forces in Iraq (MNF-I) and U.S. personnel are being observed by elements of the Jaysh al-Mahdi (JAM) and various Iranian surrogates at Basrah International Airport (BIA). As of early April, four employees of BIA reported to a JAM member, who is also an Iranian Islamic Revolutionary Guard Corps (IRGC) proxy, information on U.S. forces, translators, females, vehicles, vehicular movement, aircraft arrivals/departures, equipment, distances between various camps on the installation, and Iraqi Air Force officers. GPS-equipped Nokia N-95 smartphones were used to collect coordinates throughout the installation as well.

¶12. (S//NF) DS/TIA/ITA assesses it is plausible JAM may be planning IDF attacks directed against BIA, based on the sources having access to Nokia N-95 cell phones. According to a body of reports, the use of the N-95 is a standard tactic, technique, and procedure for such groups; Shi'a militants and sources throughout Iraq have used the GPS function on the N-95 to pinpoint point-of-impact coordinates on various forward operating bases near Baghdad and inside the IZ. Iranian-backed Shi'a militias in southern and eastern Iraq possess the weapons, training, manpower, capability, and intent for IDF attacks against BIA. The JAM sources may also be attempting to exploit station personnel, critical infrastructure, and the schedules of fixed- and rotary-wing flights in and out of Basrah. JAM and the IRGC could also be collecting information to assess capabilities and MNF-I troop levels at the airport.

¶13. (S//NF) DS/TIA/ITA further assesses the possibility that BIA may also have been infiltrated by other Iranian and IRGC surrogates. According to multiple-source reporting, the IRGC maintains an infrastructure of Iraqi officials and ideological/religious sympathizers, allowing it unfettered placement and access throughout southern and eastern Iraq. The use of Shi'a militias further provides Iran with a degree of influence against the U.S., as well as a level of plausible deniability. (Appendix sources 1-5)

¶14. (U) Significant Events

¶15. (SBU) EUR Cyprus - Emergency Action Committee (EAC) Nicosia convened April 28 to review the security arrangements for the Independence Day event (usually held July 4) scheduled for May 13 at the U.S. Chancery. Approximately 800 to 1,000 guests are expected to attend the event. Host-nation police indicated they will provide additional security assets as the RSO requested. EAC members agreed the security measures provided for the event will be adequate given the current threat environment. The EAC will monitor the security environment and initiate necessary countermeasures should a specific threat arise. (Nicosia 0291)

¶16. (SBU) AF Lesotho - A lone suspect armed with a folding pocket knife entered the Deputy Chief of Mission's residence (DCR) in Maseru May 4. The DCR is adjacent to the U.S. Embassy compound. The DCM's family was at home at the time, but the DCM was still in the Chancery. No one was injured in the incident. The man never threatened the family; he claimed to be on the run from the military police and requested clean water and a safe place to hide. The Local Guard Force (LGF) and RSO detained the suspect until local police authorities arrived. (RSO Maseru Spot Report)

¶17. (S//NF) Madagascar - EAC Antananarivo met April 30 to review the U.S. Embassy's Ordered Departure status. The committee noted that five of eight reverse tripwires have been crossed; however, the EAC recommended the status not be lifted. The EAC also reviewed the current security situation after the April 29 arrest of Ravolomanana's de facto Prime Minister (PM) Manandafy Rakotonirina and other "legalist" figures. Post will monitor the situation for a backlash to the arrests. Members noted that while there is no direct threat against U.S. interests, the EAC remains concerned about another possible downward spiral in the public security situation in Antananarivo. (Appendix source 6)

¶18. (S//NF) Sudan - The FBI received a call April 21 from an individual in Khartoum claiming he had information regarding imminent terrorist attacks planned in the United States. The caller stated Somali extremists were planning to depart Khartoum for the U.S. on April 22 to carry out the attacks. The individual met with RSO Khartoum; however, portions of his story were not credible. Based on the seriousness of the allegation, the information was shared with Khartoum's National Intelligence and Security Services for further evaluation. Post awaits the results. (Appendix source 7)

¶19. (SBU) EAP Indonesia - Approximately 100 individuals from a variety of Indonesian non-governmental organizations gathered May 3 in front of the U.S. Consular Agency in Denpasar, Bali, protesting against the Asian Development Bank (ADB) conference held in Nusa Dua, Bali, from May 2 to 5. Though the demonstration was peaceful, the Consular Agency was closed temporarily. Indonesian National Police officers monitored the event; there were no arrests or damage to USG property. On May 5, around 50 people from the group gathered at the Consular Agency. The demonstration was peaceful, but, again, Post was closed temporarily. The demonstration concluded at around 11 a.m., at which time the Consular Agency was reopened. The RSO is closely coordinating with local police and the Consular Agency regarding the possibility of demonstrations today, May 5, the final day of the ADB conference. (RSO Surabaya Spot Report)

¶20. (SBU) SCA Nepal - EAC Kathmandu convened May 4 to discuss the political and security situation surrounding the May 3 announcement of the dismissal of the chief of army staff by the PM. Due to the potential of celebratory reactions and/or protests as a result of the PM's decision, the U.S. Embassy sent out a Security Notice restricting travel and instructing Embassy employees to remain at their residences for the remainder of the day. A Warden Message was also released. There were incidents of crowds burning tires in the streets and reports of minor clashes between opposing groups; however, no injuries were reported. As of Monday morning, May 4, Nepali police had been placed on alert, but the situation was relatively calm. Subsequent to Post's EAC meeting, the PM announced his resignation, and Maoists held an uneventful rally in the afternoon. As a precaution, the American school released students early, and the American Recreation Club, which is in proximity to the rally epicenter, closed for the day. Another Maoist rally is scheduled today, May 5. Post officials will continue to monitor the situation and make adjustments to the Mission's security posture as appropriate, should the situation warrant. (See the Trends & Analysis section for further details on the situation in-country.) (Kathmandu 0363)

¶21. (U) Key Concerns

¶22. (S//NF) AF Kenya - Al-Shabaab leader allegedly deploys suicide bombers to Nairobi: Allegedly, al-Shabaab leader Fu'ad Shongale had trained and dispatched two suicide bombers to Nairobi and Mogadishu, Somalia, for possible attacks against unspecified targets in each city. According to information provided by the Canadian Security and Intelligence Service (CSIS), Shongale and al-Shabaab leader Mukhtar Robow met in mid-April at the Bakara Market in Mogadishu. There, Robow revealed his intent to significantly increase the violence targeting the Somali Government while Shongale disclosed his plan to target Nairobi and Mogadishu. Both suicide bombers were allegedly awaiting final instructions. There is no further information on the exact timing, method, location, or target of the attacks.

¶23. (S//NF) DS/TIA/ITA notes this information cannot be immediately substantiated and that the CSIS has a limited record of credible reporting in Somalia and the Horn of Africa. Although reporting continues to emerge about al-Shabaab attack planning in Kenya, the group has not successfully launched any attacks outside of Somalia, and it is unlikely it maintains the capability or desire to attack in-country at this time. (Appendix source 8)

¶24. (S//NF) Mali - AQIM discusses kidnapping Westerners: Allegedly, in early May, two al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) associates met with members of the Awlad Ghanam Faction of the Berbiche tribe to discuss the possibility of kidnapping Western hostages in the Sahel and selling them to AQIM. Specifically, the two operatives -- Hussein Ag Didi and Meide Ould Ineigh -- desired to conduct the kidnappings in order to benefit from AQIM's desire to raise money by ransoming Westerners, according to information provided by the Mauritanian Intelligence Service. Both Didi and Ineigh believed AQIM would require paid intermediaries to conduct negotiations for any kidnappings and that they would be involved in the negotiations and make a profit. The two operatives also desired to benefit from AQIM's anger over the arrest of four of its operatives by Malian authorities on April 26.

¶25. (S//NF) DS/TIA/ITA notes local militia/bandits kidnapped two Canadians and four Europeans in the Sahel in December 2008 and January, respectively, and sold them to AQIM. The late-April exchange of four of those hostages for three AQIM prisoners and a ransom may prompt other nefarious elements throughout the Sahel to continue targeting Westerners for abductions. After spending the money gained by the ransom of two Austrian hostages in October 2008, AQIM offered a bounty for kidnapped Westerners in late 2008. In response, local bandits kidnapped the two Canadians in Niger and the four Europeans. It is possible rogue elements in the Sahel will kidnap any Westerners in hopes of being paid by AQIM, even if the group does not need hostages at the time.

¶26. (S//NF) Meanwhile, the arrest of the four AQIM operatives in late April may also prompt the group to kidnap Westerners. Both Abu-Zaid and Belmokhtar have expressed anger over the arrests; although, it remains unclear what role the four operatives played in the group. If the four recently arrested operatives prove critical to either Abu-Zaid or Belmokhtar, they may ask associates in the region to kidnap Westerners in order to exchange them for the detainees. Indeed, the August 31, 2008, arrest of two of Belmokhtar's operatives -- both of whom were critical to an unidentified "project" he was leading -- was another factor that led AQIM to release the bounty offer. (Appendix sources 9-11)

¶27. (SBU) Nigeria - On May 4, RSO Lagos and DS/TIA/OSAC coordinated and passed the following tearline to a named U.S. company. "Allegedly, an attack may be imminent against the (named company) Utorogu Gas Plant in Ughelli South Local Government Area. Allegedly, a group named the Ughievwen Youth Body Fighters threatened an attack if certain demands were not met. There is no further information as to the exact timing, method, location, or target of attack." The company was unaware of the threat and did not have any immediate feedback. (DS/TIA/OSAC)

¶28. (S//NF) NEA Yemen - ROYG offers truce to extremist community: According to information obtained from former al-Qa'ida in the Arabian Peninsula (AQAP) commander Muhammad al-Harbi and provided by the Saudi Mabahith, the Republic of Yemen Government (ROYG) supposedly offered a truce to AQAP in early February. Yemeni Political Security Organization Director General al-Qamish reportedly tasked an individual to extend the truce to AQAP Emir Nasir al-Wahishi, who then claimed he was not the decision-maker and that an answer would be returned in days if the group accepted. The ROYG offered to cease attacks on AQAP if the organization halted attacks against ROYG elements, yet no further contact occurred -- suggesting AQAP did not accept the truce. The Mabahith notes al-Wahishi's hesitancy to commit to an answer unilaterally likely illustrates wanted Egyptian al-Qa'ida affiliate and current AQAP member Ibrahim al-Banna's role in providing guidance and strategic direction to the AQAP organization.

¶29. (S//NF) DS/TIA/ITA notes earlier reporting on the alleged truce offered by President Salih reported by a source with contacts in the Yemeni extremist community. It is highly likely Salih did indeed offer the truce, as recent information strongly suggests Salih's most pressing concern remains preserving his own power rather than eradicating Yemen's thriving extremist community. AQAP's rejection of the cease-fire highlights the already permissive security environment; AQAP leadership is aware even should ROYG security forces continue their counterterror campaign, such actions are unlikely to significantly affect operational planning and/or execution. President Salih's consideration of the political oppositionist movement as the priority threat to his regime strongly suggests the ROYG will continue attempts to appease or even co-opt extremist elements while attempting to quell secessionist sentiment in the south. Following this strategy, Yemeni counterterrorism operations against AQAP will likely wane, and the extremist organization will have even more freedom to plot attacks in both Yemen and in neighboring Saudi Arabia. (Appendix sources 12-13)

¶30. (S//NF) SCA Afghanistan - Iranian MOIS tasking source to determine how to attack U.S. contractor facility: A sensitive source citing secondhand access reported that as of mid-April, the chief of security for the Ministry of Intelligence and Security (MOIS) in Taybad, Iran, tasked a source to obtain information on USG facilities. He specifically discussed how to attack a named U.S. contractor facility in Islam Qala, Herat, using a vehicle with explosives.

¶31. (S//FGI//NF) DS/TIA/ITA notes this threat information is likely referencing early-February reporting detailing plans by Taliban commander Mullah Sangin to attack vehicles belonging to a named U.S. contractor near its base in Islam Qala, Kuhestan District, Herat Province, with suicide vehicle-borne improvised explosive devices. Separate reporting from early May indicates Mullah Sangin threatened to attack unspecified Western foreigners at the Islam Qalah border crossing in Kuhestan District. Earlier reporting suggests members of the Iranian Revolutionary Guard Force may provide Mullah Sangin with financial support and weapons to engage Coalition forces. Although the exact nature and degree of support to insurgent elements remains unclear, Iran's strategy in Afghanistan focuses on fomenting discord within the country to create security problems for the U.S., thus rendering it unable to focus on Iran.

¶32. (S//FGI//NF) Mullah Sangin (Terrorist Identities Datamart Environment number 235742) is a senior Taliban field commander in Herat Province reportedly responsible for orchestrating suicide attacks. Reporting from the Afghan National Directorate of Security in mid-2007 also indicated Sangin previously sought to target USG contractors as they entered or exited the Afghan National Police Regional Training Center in Herat city. Sangin has been tied to at least one suicide bombing in Herat Province. He was reportedly responsible for the January 30, 2007, attack in Herat city when a bomber drove an explosives-laden vehicle into an Afghan army bus, killing five and injuring 10 soldiers and two civilians. (Appendix sources 14-21)

¶33. (U) Threats & Analysis

¶34. (S//NF) SCA Nepal - Overview of recent events: The May 3 dismissal of Nepal's chief of army staff (COAS) by the Maoists, the subsequent withdrawal of the Communist Party of Nepal-Unified Marxist Leninist (CPN-UML) from the Maoist-led government, and the May 4 resignation of PM and Maoist leader Pushpa Kamal Dahal (a.k.a. Prachanda) have brought into question the durability of the 2006 Peace Agreement and raised the specter of a renewal of the violence from the 1996 to 2006 civil war. Although it is too early to definitively determine the course of these fluid events, both the Maoists and opposition parties have promised to launch protests in reaction to the high-level political events, raising the distinct possibility of outbreaks of violence fueled by the activities of political youth gangs.

¶35. (S//NF) Although the latest move by the Maoists to force the COAS from power has cost them the support of the CPN-UML, the Maoists remain the most organized force in the country and in the past have repeatedly secured their political demands through mass protests and strikes. This track record has likely figured into the Maoists' calculus of risking political isolation with securing the demands of the rank and file to be integrated into the army. Although there are no signs at the present time suggesting the Maoists intend to abandon their place in government, the group's youth wing -- the Young Communist Democratic League (YCDL) -- remains a potent force with a long history of orchestrating effective intimidation campaigns. While less organized, other political groups such as the CPN-UML have formed "combat" youth wings following the Maoists' ascendance to political power, presumably to compete with the Maoist YCDL and setting the stage for potentially violent confrontations during public protests. The army's reaction to a sustained public agitation campaign by the Maoists, however, remains much more unclear. Regional media analysis has speculated the army may seek to instigate a "soft coup" similar to the January 2007 army-backed declaration of a "state of emergency" in Bangladesh following violent protests between opposing political parties. As with the Maoists, however, there are few signs the army is preparing for a return to full-blown conflict apart from an increased presence in Kathmandu.

¶36. (SBU) More generally speaking, this latest political drama is likely to slow down the already glacial pace of progress of efforts to address the country's growing list of basic needs, particularly the ability to enforce quotidian rule of law. This lack of progress continues to exacerbate security concerns highlighted by increasing numbers of protests, kidnappings, murder, and low-level bombings. Although there is no current reporting indicating Western interests are being targeted for attack, continued paralysis of Nepal's security services and the impunity with which organized gangs of all stripes can operate suggest criminality and the resultant social disaffection will continue unabated. (Kathmandu 1245; Appendix sources 22-30)

¶37. (U) Cyber Threats

¶38. (U) Worldwide Continued interest in hacking wireless networks:

¶39. (S//NF) Key highlights:
o Malicious actors continue to develop exploits targeting wireless network connectivity.
o Videos and discussions of hacking techniques are regularly submitted to hacker forums.
o Members of Farsi-language forums recently posted wireless exploit details.
o Increased awareness of and security for wireless technology vulnerabilities is necessary.

¶40. (SBU) Source paragraph: "A SANS (SysAdmin, Audit, Network, Security) expert who spoke at the RSA information security conference has warned that intruders do not need physical proximity to exploit security weaknesses in wireless networks. ... An attacker reportedly can conduct long-distance wireless hacks that do not require access through a wireless connection or can use wireless hacks in combination with other attacks to gain access. These types of attacks are not aimed at individual systems, but seek to attack networked environments, such as within organizations."

¶41. (SBU) CTAD comment: While becoming a significant resource for private and government organizations, wireless networks have also turned out to be easy, valuable targets and a force multiplier for malicious actors. As such, security issues stemming from the growing use of wireless connectivity continue to raise concerns for users and administrators. For example, improperly configured devices do not adequately protect data. Even properly configured wireless segments are targeted using publicly accessible tools designed to defeat specific vulnerabilities, continuing to place information at risk. Additionally, wireless networking vulnerabilities translate to threats to associated wired networks. Likewise, possible new methods of exploiting wireless networks involve first compromising wired systems through conventional social engineering and malicious software infections, whereupon attackers could use available wireless connectivity as a means to hop to other associated devices (e.g., access points and other wireless-enabled systems). This may potentially provide hackers with the ability to remotely attack multiple networks as well as offer further anonymity to their nefarious activities.

¶42. (S//NF) CTAD comment: DoD reporting indicates on July 19, 2008, "Bl4ck.Viper," a member of the Farsi-language Web forum "Delta Hacking Security Center" (deltahacking.net), posted a wireless network-hacking program. From July 20 to 30, Bl4ck.Viper exchanged comments and tips on using the program with at least three fellow hackers. The registered monikers for these associates have been identified as "Black.RiOT," "Dr.xm0r741," and "mohammad462." During the supplementary discourse, Bl4ck.Viper stated the software he provided is a combination of a number of programs (NFI), further acknowledging that the combination of programs was important because individual programs such as sniffers are not sufficient to successfully compromise wireless networks. Instead, sets of specialized tools are needed to accomplish various tasks associated with hacking wireless devices and connectivity.

¶43. (S//NF) CTAD comment: On October 16, 2008, on the same Farsi-language Web forum, another member registered as "PLATEN" posted an English-language article that contained links to a video allegedly used by the FBI regarding hacking wireless networking devices. The video specifically discusses the Wired Equivalent Privacy encryption scheme, including details of the encryption's construct as well as programs and attacks used to crack it (e.g., Aircrack). Additionally, links through which other hackers can download the video were offered on such open source file-hosting websites as the Switzerland-based "Rapidshare.com" and the Hong Kong-based "Megaupload.com."

¶44. (SBU) CTAD comment: Foreign hackers, such as the aforementioned Iranian actors, continue to express an interest in acquiring tools designed to facilitate hacking operations against wireless networks. In addition, tech-savvy groups such as the Indian Mujahideen -- whose members have received training on wireless hacking and have implemented sophisticated techniques in support of terrorist attacks -- also seek to develop hacking proficiency and methodologies. Aiding these efforts are an increasing availability of information and numerous ways for malicious actors to share resources. Lapses in security, as well as users' lack of understanding of the threats to networks, also continue to put information at risk for exploitation or corruption. Therefore, for situations in which wireless-enabled systems are present, a multilayered or defense-in-depth approach in conjunction with extensive user training must be applied in order to best mitigate potential threats and help prevent network compromises.

¶45. (U) CTAD comment: In accordance with the Foreign Affairs Manual (5 FAM 580), the following policies have been established to regulate the use of wireless networking technologies throughout DoS facilities.
¶1. Connecting personally owned devices to DoS systems or networks is prohibited.
¶2. Wireless networking devices must be disconnected/powered off when not in use, and wireless and wired connections may not be simultaneously operational.
¶3. DoS facilities must coordinate with the appropriate Regional Information Management Center, Regional computer security officer, the Office of Security Technology, and the Office of Computer Security regarding the configuration, installation, and operation of wireless networks.
¶4. Data must be encrypted using National Security Agency (NSA)- and National Institute of Standards and Technology-approved products, which must also be NSA endorsed and approved by the Information Technology (IT) Change Control Board.
¶5. Connecting wireless networking devices to classified information systems is prohibited, and wireless-enabled devices may not process or store classified information.
¶6. Loss, theft, or any other security-related situation involving wireless IT devices must be reported to the information systems security officer (ISSO) and unit security officer. For additional information regarding wireless networking, see CTAD Report 08-014. (Appendix sources 31-32)

¶46. (U) Suspicious Activity Incidents

¶47. (SBU) EUR roatia - A man with a bicycle stood on an overpass located 200 meters from U.S. Embassy Zagreb May 4. From his location, the subject had a clear view of the access road and main intersection leading to Post. The subject had a camera on the bicycle seat facing toward the Embassy. The LGF and Surveillance Detection Team (SDT) were advised of the incident, but, by the time they arrived, the subject had left. (SIMAS Event: Zagreb-00166-2009)

¶48. (SBU) AF Eritrea - A man stood 50 meters from U.S. Embassy Asmara May 2. Upon interdiction, the subject told police he was waiting for a resident who lives next door to the Embassy to return home so he could talk to him about working for his company as a driver. Police told the subject to move on, and he complied.

¶49. (SBU) RSO Action/Assessment: The RSO is treating this incident as suspicious and has passed information on the subject to LGF and SDT assets. The foreign service national investigator will talk to the neighbor to ascertain if he knows the man. The RSO submitted the subject's name for checks with the police and the Embassy.

¶50. (SBU) Record Check/Investigation: Subject: Ebrahim Ata. DPOB: 1936; Asmara. Identification number: 0115465. (SIMAS Event: Asmara-00730-2009)

¶51. (SBU) NEA Jordan - An individual parked his vehicle near U.S. Embassy Amman residences April 30. The vehicle departed and returned a few minutes later. On a third sighting, the vehicle was vacant. Police were notified, but, when they responded, the vehicle was gone. A BOLO was issued.

¶52. (SBU) RSO Action/Assessment: The RSO has requested police investigate this event.

¶53. (SBU) Record Check/Investigation: Vehicle: Dark-blue Mitsubishi Lancer; License plate: 16-68775. (SIMAS Event: Amman-03646-2009)

¶54. (SBU) Oman - A man photographed the perimeter wall around the Chief of Mission residence in Muscat May 3. The local guard stopped the subject and called police. Police detained the subject and took him to the station for further questioning. The RSO office will follow up with the police.

¶55. (SBU) Record Check/Investigation: Subject: Mbwoge Martin Mullor. Citizenship: Cameroon. Identification number: ¶9309272. According to the subject's immigration stamp, he has been in Oman for three days. (SIMAS Event: Muscat-00129-2009)

¶56. (SBU) Saudi Arabia - A man appeared at the U.S. Embassy Riyadh main gate May 4. He seemed to be studying Post's access and exit locations. Police interdicted; the subject indicated he is a Syrian national and was waiting for his friend who was at the Embassy (NFI). (SIMAS Event: Riyadh-00243-2009)

¶57. (SBU) Tunisia - On April 30, a man stood near the entrance to the road leading to the U.S. Ambassador's residence in Tunis. The subject was in the area for about 20 minutes, walking back and forth while talking on a cell phone. During this time, the Ambassador departed the residence (NFI). (SIMAS Event: Tunis-02019-2009)

¶58. (SBU) United Arab Emirates - A man sat and walked around the area of a car park located near U.S. Consulate General Dubai April 30. During this time, the Consul General (ConGen) arrived at Post, and the subject remained for an hour before leaving.

¶59. (SBU) RSO Action/Assessment: This appears to be surveillance activity. It is not known if the ConGen was the target or the nearby Trade Center environs. The SDT was notified, and the LGF was briefed on the event. If the subject is seen again, the RSO will request police assistance. (SIMAS Event: Dubai-00182-2009)

SECRET//FGI//NOFORN

Full Appendix with sourcing available upon request.
CLINTON